UNITED STATES MARINE CORPS
MARINE CORPS OPERATIONAL TEST AND EVALUATION ACTIVITY
3035 BARNETT AVENUE
QUANTICO, VIRGINIA 22134-5014

IN REPLY REFER TO:

MARCORSYSCOM
5000
Ser
14 Jun 02

MCOTEA
5000
Ser
20 MAY 2002

MEMORANDUM OF UNDERSTANDING
BETWEEN
COMMANDER, MARINE CORPS SYSTEMS COMMAND
AND
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND EVALUATION ACTIVITY

Subj: OPERATIONAL TEST AND EVALUATION (OT&E) OF SECURITY, JOINT INTEROPERABILITY, ELECTROMAGNETIC ENVIRONMENTAL EFFECTS/SPECTRUM MANAGEMENT (E3/SM) AND INFORMATION ASSURANCE (IA)

Encl: (1) References
(2) Acronym List

1. Purpose. This Memorandum of Understanding (MOU) is established to clearly define how the Marine Corps Systems Command (MARCORSYSCOM) and the Marine Corps Operational Test and Evaluation Activity (MCOTEA) will coordinate efforts to test and evaluate security, Joint Interoperability, E3/SM, and IA.

2. Scope. This MOU applies to all systems to be employed by the United States Marine Corps (USMC) operating forces that are required to conduct assured, secure and interoperable Information Operations (IO). These systems fall into two categories:

a. Systems being developed by MARCORSYSCOM and tested by MCOTEA.

b. Systems jointly developed in conjunction with other services for which the lead developing and/or testing agency may be from another service.

3. Background. DoD Joint Vision-2020 emphasizes the importance of Network Centric Warfare (NCW). NCW relies on distributed platforms and sensors to detect, locate, target, and eliminate enemy with precision munitions. The effective

conduct of NCW is dependent upon effective IO. IO is defined as actions taken to affect adversary information and Information Systems (IS) while defending ones own information and IS. IA is a subset of IO that protects and defends information and IS by ensuring their availability, integrity, confidentiality, authentication and non-repudiation. IA includes providing for restoration of IS by incorporating protection, detection and reaction capabilities into those systems. Without effective IA, the smart enemy will attempt to disrupt the network, isolate sensors from weapon systems, and render the fighting force ineffective. A more sophisticated enemy will attempt to infiltrate the network and exploit it against the friendly fighting force.

The emerging challenge for developers is to procure and field systems that incorporate effective IA capability. IA is more than just system security. Granted, system security does touch all aspects of IA including availability, integrity, confidentiality, authentication, and non-repudiation. IA is also directly related to other system characteristics, including Joint Interoperability and E3/SM. Service and Joint Interoperability requirements establish the context within which we execute IO and evaluate IA posture. E3/SM impacts the availability and integrity of IO. Radio frequency spectrum is often required to execute IO and must be reserved, available, and managed.

4. Policy and Guidance. References (a) through (z), listed in enclosure (1), provide specific policy, guidance, and levy requirements on developers and testers regarding Security, Joint Interoperability, E3/SM, and IA. Proper compliance with this guidance and policy is critical in order for a system to achieve threshold Operational Effectiveness (OE) and Operational Suitability (OS) requirements. With so many pertinent references, the challenge is to understand the policy and guidance, recognize the interrelationships between them, and devise a thorough acquisition and test strategy that supports the policy and guidance. Security, Joint Interoperability, E3/SM, and IA are critical system characteristics that are interrelated and must be evaluated collectively. The goal is to leverage the acquisition process to minimize the cost of testing and achieve timely fielding of secure, interoperable systems. It is important to emphasize that Title 10 United States Code allows independent Operational Testing Agencies to leverage activities and testing

conducted by other agencies provided appropriate Government oversight has been applied.

The IA strategy addressed here has been developed based on Director of Operational Test and Evaluation (DOT&E) policy for OT of IA (references (a) and (b)). The DOT&E policy has since been incorporated into the DoD 5000.2-R, reference (c). This strategy relies heavily on the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) discussed in references (d), (e) and (f). References (g) and (h) also address security and are listed in enclosure (1) for completeness. Joint Interoperability and E3/SM also impact IA posture. The Chairman Joint Chiefs of Staff Instruction (CJCSI) 3170.01 and CJCSI 6212.01 references (i) and (j), are key documents that provide Joint Interoperability guidance. Reference (k), Marine Corps Order 3093.1C, provides specific USMC guidance on inter and intraoperability of National Security Systems and IT systems. References (l), (m), (n) and (o) also address interoperability and again are listed in enclosure (1) for completeness. Several documents provide guidance for E3/SM including references (p), (q), (r) and (s). IA is addressed in references (a), (b), (t), (u) and (v).

5. Coordinating OT&E for IA. Key participants in the OT&E for IA process are the Program Manager (PM), Project Officer (PO), Operational Test Project Officer (OTPO), DITSCAP Certification Authority (CA), and DITSCAP Designated Approving Authority (DAA). Procedures for planning executing, and reporting for OT are addressed in SECNAVINST 5000.2, the USMC Acquisition Procedures Handbook of 1996, the MCOTEA Standard Operating Procedure of September 2000, and the Memorandum of Agreement for Multi-Service OT&E of May 2001, references (w), (x), (y) and (z).

The OT&E planning process begins with the identification of a new program. Up front and early identification facilitates coordination and can help to minimize costs and maximize results. The MARCORSYSCOM Project Officer (PO) will establish a Test Integration Working Group (TIWG) to coordinate planning. The TIWG provides a forum through which MARCORSYSCOM and MCOTEA remain actively involved in the Security Certification and Accreditation process and can also coordinate Joint Interoperability, E3/SM, and IA testing. The Joint Interoperability Test Command (JITC) and Marine Corps Tactical Systems Support Activity (MCTSSA) may be invited to participate in the TIWG. Every effort will be

made to exploit the Systems Integration Environment (SIE) at MCTSSA to support testing. Continuous communication throughout the TIWG meetings will maximize opportunity to leverage testing efforts to ensure success.

The Test and Evaluation Master Plan (TEMP) documents planning and serves as a "contract" between MARCORSYSCOM and MCOTEA. The TEMP documents Developmental Test (DT) and OT activities planned to satisfy Joint Interoperability, Security, E3/SM, and IA requirements. The TEMP Part III should address Security, Interoperability, and E3/SM DT plans. The TEMP Part IV will describe how data provided from Joint Interoperability, Security, E3/SM DT will be evaluated. If required, the TEMP Part IV will address supplemental Joint Interoperability, Security, E3/SM OT testing. Part IV will also address IA OT plans. The TEMP Part V should identify resources and funding requirements for MCOTEA, MCTSSA, and JITC, as required.

For joint systems/programs, JITC may produce a Joint Interoperability Test Plan. This test plan is distinct from the TEMP and provides the context within which IO are executed. The infrastructure required to conduct Joint Interoperability testing can concurrently support Security, E3/SM, and IA OT.

The DITSCAP requires creation of a Certification Test and Evaluation (CT&E) Plan and a Security Test and Evaluation (ST&E) Plan, which are also distinct from the TEMP. The CT&E plan is developed to support certification testing in a development environment, while the ST&E is developed to support security testing in an operational environment. Security Test Reports document the residual risks that remain with the system after all countermeasures are implemented.

E3/SM testing is typically executed as part of the overall DT effort. DOT&E provides an excellent E3/SM Assessment Guide, reference (r) that can be used shape the E3/SM programs. E3/SM risk should be mitigated as part of the development process and quantified before OT.

The PO must also allocate frequency spectrum, as documented in a DD-1494 from the Service Frequency Management Office (FMO) and coordinate Host nation Frequency Supportability.

6. Leveraging Key Acquisition Products. The products of Joint Interoperability, Security, E3/SM and Security Process produces during DT, will be used by MCOTEA to comprehensively evaluate IA effectiveness. These products provide MCOTEA with data that can be used to help determine remaining residual IA risk, and thus OE and OS. The acquisition products that will be used are listed below. The individual or organization listed in parentheses identifies who is responsible for the development and/or approval of the listed product. The following key acquisition products will be used to determine residual IA risk:

a. Security: System Security Authorization Agreement (PO)

b. Security: Vulnerability Assessment (CA)

c. Security: Interim Authority to Operate/ Authority to Operate (DAA)

d. Interoperability: J-6 Interoperability Requirements Certification i.e. Approved Operational Requirements Document with Operational View 1, System View 1 and Information Exchange Requirements (Joint Staff J-6)

e. Interoperability: C4ISP Supportability Certification (Joint Staff J-6)

f. Interoperability: JTA Compliance Certification (Defense Information System Agency or component as appropriate)

g. Interoperability: Interoperability Test Certification (JITC)

h. Interoperability: Interoperability System Validation (Joint Staff J-6)

i. E3: Intra Platform/System Analysis (PO)*

j. E3: Inter Platform/System Analysis (PO)*

k. E3: E3 Impact Assessments (PO)*

l. E3: Military Standard (MIL STD) 461/464 Reports or equivalent (PO)*

m. SM: DD-1494 Approved with Spectrum Certification (PO)*

n. SM: Status of Host Nation Frequency Supportability (PO)

*See Reference (r) DOT&E E3/SM Assessment Guide for OT

7. Roles and Responsibilities. The following roles and responsibilities are assigned:

a. MARCORSYSCOM (PM and PO). Reference (y) identifies MARCORSYSCOM as the primary Developing Agency (DA) for the USMC. MARCORSYSCOM is responsible for developing systems that meet the operational requirements established by the Marine Corps Combat Development Command (MCCDC) and other DoD Directives (DoDD) where appropriate. MARCORSYSCOM may collaborate with other developing agencies to jointly procure a system. As discussed in reference (y), the PO is MARCORSYSCOM's representative responsible for overall program execution and DT planning, execution and reporting. The MARCORSYSCOM PM and/or the PO are responsible for the following activities:

(1) The MARCORSYSCOM PM will formally notify the Director of MCOTEA of new programs that require OT.

(2) The MARCORSYSCOM PM will designate a PO to conduct the day-to-day liaison and coordination with the OTPO, JITC, MCTSSA, DAA, CA, and Frequency Management Office as appropriate.

(3) For programs where MARCORSYSCOM is a member of a multi-service acquisition team lead by another service, the PO will coordinate with the lead DA, DAA, and the MCOTEA OTPO to ensure appropriate IA related development activities are initiated so they may be leveraged to resolve Joint Interoperability, Security, E3/SM, and IA issues.

(4) The PO will establish a TIWG.

(5) The PO will develop a TEMP, which will document Joint Interoperability, Security, E3/SM activities in Part III of the TEMP. Resources required by MCOTEA, MCTSSA, JITC, and other activities must be addressed in Part V of the TEMP.

(6) The PO will coordinate as appropriate with the CA and Component CIO to determine the system's mission category per references (t), (u) and/or (v).

(7) The PO will coordinate with the Joint Staff J-6, DISA and JITC as appropriate to achieve Joint Interoperability Requirements.

(8) The PO will execute the security process, (DITSCAP). This includes registering the system with the DAA, developing a Systems Security Authorization Agreement (SSAA), and providing vulnerability assessments and security documentation as appropriate.

(9) The PO will develop and execute an E3/SM test plan and ensure frequency spectrum is allocated via DD-1494 and that Host Nation Frequency Supportability is obtained, per the process described in the (DOT&E) E3/SM guidance in reference (r).

(10) The PO will provide results of Joint Interoperability, Security, and E3/SM testing to MCOTEA. The PO will ensure all data is provided to the MCOTEA OTPO with sufficient time to report status as part of the Operational Test Readiness Review (OTRR).

Certification Authority (CA). The CA will be designated by MARCORSYSCOM. The CA is responsible for making a technical judgment regarding the system's compliance with security requirements. As such, the CA is responsible for the following activities:

(1) Participate as a member of the TIWG, as appropriate.

(2) In conjunction with the PO and OTPO, develop security test plans. Document security test plans in Part III of the TEMP. Identify to the PO all resources required for security testing and ensure resources are included in Part V of the TEMP.

(3) Develop CT&E and ST&E plans, and execute and report on such plans. Report security test results and include a vulnerability assessment and residual risk assessment. (The certification authority may accomplish

security testing through a Certification Agent, a person, or organization that actually conducts the testing.)

(4) Ensure all data are provided to the PO and OTPO with sufficient time to report status to support the Operational Test Readiness review (OTRR).

(5) Make a technical recommendation regarding Interim Authority to Operate (IATO) and Authority To Operate (ATO) to the DAA.

c. DAA. The DAA will be designated by MARCORSYSCOM. The DAA is responsible for the following activity:

(1) Provide the IATO, ATO or denial for newly certified systems on USMC networks based on a technical recommendation from the CA.

d. MCOTEA (OTPO). Reference (w) designates MCOTEA as the independent OTA for the USMC. In some cases, MCOTEA will serve as the lead service OTA for Multi-Service OT&E or serve as a supporting service OTA as part of a Multi-Service Test Team (MTT). The OTPO is MCOTEA's representative responsible for OT&E planning, execution, and report generation. As discussed in reference (y), the MCOTEA OTPO is responsible for the following activities:

(1) Upon notification of a new program by the MARCORSYSCOM PM, the Director of MCOTEA will designate an OTPO, who will conduct the day-to-day liaison with the PO, JITC, CA, and MCTSSA as appropriate.

(2) Where MCOTEA is a member of a MTT led by another OTA, the OTPO will coordinate with the lead service OTA's designated test director and the MARCORSYSCOM PO to ensure appropriate testing data is used to resolve IA OT test issues.

(3) As a member of the TIWG, in coordination with the PO, JITC, CA, and MCTSSA, will develop an IA OT&E strategy as part of the overall OT&E planning process.

(4) Generate a comprehensive TEMP Part IV that, in addition to program specific testing, addresses Joint Interoperability, Security, E3/SM and IA OT. Document how data provided from Joint Interoperability, Security, E3/SM DT will be evaluated. Address supplemental Joint

Interoperability, Security and E3/SM OT if required and document the planed IA OT&E strategy. The OTPO will identify to the PO any resources required for the conduct of IA OT in Part V of the TEMP. This may include resources to execute dedicated "Red Team" Penetration Testing if required.

(5) Assess the level of IA risk and coordinate to leverage DT data from Security, Joint Interoperability, and E3/SM testing to resolve that risk.

(6) Attend, or send a designated representative to observe DT events to satisfy Title 10 requirements as required.

(7) Upon review of DT data, conduct dedicated IA OT&E, if appropriate, based upon the level of residual risk identified through the DT process.

8. Test Data Sharing. In some instances, test results and reports will be classified and protected according to the level of classification. MARCORSYSCOM and MCOTEA agree to safeguard each other's test data and the release of such data to third parties shall be per established procedures of the data owner. Per Title 10 restrictions and reference (z), the MCOTEA OTPO will not release any test data without the explicit approval of the Director of MCOTEA.

9. Resources. Reference (w) states MARCORSYSCOM will provide funding required for the conduct of test. The activity conducting that test is responsible for managing those funds. Funds required by MCOTEA, JITC, CA, MCTSSA and other activities will be addressed in Part V of the TEMP and coordinated and agreed to by all concerned agencies.

10. Amendments and Termination

a. The Commander, MARCORSYSCOM or Director of MCOTEA may propose changes to this MOA, for mutual agreement, when needed by either party.

b. This MOA may be terminated at either party's discretion within 90 days written notice.

11. Effective Date. This MOU is effective when signed by both parties.

W. D. Johnson
Colonel, USMC
Director

20 May 2002
Date

J. M. Feigley
Brigadier General, USMC
Commander

6/14/02
Date

References

a. DOT&E Policy for Operational Test and Evaluation of Information Assurance of 17 November 1999

b. DOT&E Guidelines on Metrics for Operational Testing of Information Assurance of 19 January 2001

c. DOD 5000.2-R Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs of March 2002

d. DoDI 5200.40 DoD Information Technology Security Certification and Accreditation Process of 30 December 1997

e. DoD 8510.1-M; Department of Defense Information Technology Security Decertification and Accreditation Process; Application Manual of 31 July 2000

f. USMC Project Officer's Certification and Accreditation Handbook Version 3.0 of September 2000

g. DoDD 5200.28 Security Requirements for Automated Information Systems of 21 March 1988

h. SECNAVINST 5239.3; Department of the Navy Information Systems Security Program of 14 July 1995

i. CJCSI 3170.01A Requirements Generation System of 15 April 2001

j. CJCSI 6112.01B Interoperability and Supportability of National Security Systems and Information Technology Systems of 8 May 2000

k. MCO 3093.1C; Intraoperability and Interoperability of Marine Corps Tactical C4I Systems of 15 June 1989

Encl (1)

l. OSD Promulgation of Information Technology Interoperability of 4 December 2000

m. Deputy Secretary of Defense Memorandum on Command and Control Legacy Interoperability Strategy and Milestone Action Plan of 12 October 2001

n. DoD Directive 4630.5, Interoperability and Supportability of Information Technology and National Security Systems of 11 January 2002

o. DoDI 4630.8 Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems of 18 November 1992 (Under Revision)

p. DoDD 3222.3; Department of Defense Electromagnetic Compatibility Program of 20 August 1990

q. OPNAVINST 2450.2; Electromagnetic Compatibility Program within the Department of the Navy of 8 January 1990 DOT&E Policy on Operational Test and Evaluation of E3/SM of 25 October 1999

r. DOT&E Electromagnetic Environmental Effects/Spectrum Management Assessment Guide for Operational Testing of 13 July 2001

s. OPNAVINST 2400.20E; Navy Management of the Radio Frequency Spectrum of 19 January 1989

t. DOD CIO Global Information Grid Information Assurance Policy Memorandum No. 6-8510 of 16 June 2000

u. DoDD 8500.aa, Information Assurance (in Draft)

v. DoDI 8500.bb, Information Assurance Implementation (in Draft)

w. SECNAVINST 5000.2B Implementation of Mandatory Procedures for Major and Non Major Defense Acquisition Programs and Major and Non Major Information Technology Programs of 6 December 1996 (Under Revision)

y. U.S. Marine Corps Acquisition Procedures Handbook; (Includes Change 1 of 16 February 2000) of September 1999

x. Marine Corps Operational Test and Evaluation Activity Standing Operating Procedures with Change 2 dated 17 January 2002

z. Multiservice Operational Test and Evaluation Memorandum of Understanding of May 2001

Acronym List

ATO	Authority to Operate
CA	Certification Authority
CJCSI	Chairman Joint Chief of Staff Instruction
CT&E	Certification Test and Evaluation
DA	Developing Agency
DAA	Designated Approving Authority
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DOT&E	Director of Operational Test and Evaluation
DT	Developmental Testing
E3/SM	Electromagnetic Environmental Effects/Spectrum Management
FMO	Frequency Management Office
IA	Information Assurance
IATO	Interim Authority to Operate
IO	Information Systems
IS	Information Systems
JITC	Joint Interoperability Test Command
KPP	Key Performance Parameter

MARCORSYSCOM	Marine Corps Systems Command
MCCDC	Marine Corps Combat Development Command
MCOTEA	Marine Corps Operational Test and Evaluation Activity
MCTSSA	Marine Corps Tactical Systems Support Activity
MOU	Memorandum of Understanding
NCW	Network Centric Warfare
NSS	National Security Systems
OE	Operational Effectiveness
OS	Operational Suitability
OT	Operational Testing
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTPO	Operational Test Project Officer
PM	Program Manager
PO	Project Officer
ST&E	Security Test and Evaluation
TEMP	Test and Evaluation Master Plan
TIWG	Test Integration Working Group
USC	United States Code
USMC	United States Marine Corps